Scopus

Documents

Nagy, N., Nagy, M.

Quantum bit commitment-within an equivalence class
(2016) *International Journal of Unconventional Computing*, 12 (5-6), pp. 413-432.

Abstract
Quantum bit commitment (QBC) is a fundamental cryptographic primitive that can be used as a building block for a whole set of applications like remote coin tossing, zero-knowledge proofs or secure two-party computation. Unconditionally secure QBC, that is a protocol which is both fully binding and fully concealing, is deemed impossible due to the use of entanglement by a dishonest participant [10, 14]. In this paper, we describe a protocol that implements QBC using quantum memories, meaning that a qubit can be stored for as long as needed. We prove that, in the absence of entanglement, our protocol exhibits both properties: it is both binding and concealing. Its security exploits the algebraic properties of an equivalence class with two types of operators: permutation and the Hadamard transform. The only theoretical attack that can be mounted concerns the binding property through the use of entanglement and the Schmidt decomposition. However, for all practical purposes, such an attack can be made arbitrarily difficult, by increasing the value of a security parameter, namely the number of qubits used in the protocol. © 2016 Old City Publishing, Inc.

2-s2.0-85007377854
Document Type: Article
Publication Stage: Final
Source: Scopus